Secure Computing Magazine

INDEX

AKTUEEL

Politie en wetenschap bundelen krachten bij opsporing

De Nederlandse politie gaat samenwerken met wetenschappers om de data op in beslag genomen smartphones beter te analyseren. De politie start hiervoor het project Politielab. Twee universiteiten, de Hogeschool van Amsterdam en het Centrum Wiskunde & Informatica doen hieraan mee.

Binnen het nieuwe Politielab zullen de komende maand drie onderzoekers worden aangenomen. Deze drie mensen worden door de politie gefinancierd.

Politielab werkt aan software waarmee met een druk op de knop een samenvatting kan worden gemaakt over data van alle in beslag genomen apparaten bij een onderzoek. Daarbij wordt gekeken naar relaties en afwijkende patronen in de uitgelezen gegevens.

Er moet bijvoorbeeld worden gekeken naar locatiegegevens in afbeeldingen. Door te kijken of foto's van twee smartphones rond dezelfde tijd en op dezelfde locatie zijn gemaakt, kan de software concluderen dat de telefoonbezitters samen waren.

Niet ongericht

Volgens Theo van der Plas, programmadirecteur digitalisering en cybercrime van de politie, zal de nieuwe software niet ongericht worden ingezet.

De Hoge Raad oordeelde onlangs dat een smartphone niet zonder toestemming volledig mag worden uitgelezen bij een onderzoek. Daarbij kan namelijk een bijna compleet beeld van iemands leven ontstaan. Er moet daarom toestemming worden gevraagd aan een officier van justitie of rechter-commissaris.

Volgens Van der Plas gaat Politielab voornamelijk helpen bij het doorgronden van uitgelezen data. Data die versleuteld op een telefoon is opgeslagen, is met de nieuwe software nog steeds niet uit te lezen.

Rubrieken:

- Verder op Facebook / de website
- Cops in Cyberspace
- Rechtspraak
- Verschijningsvorm cybercrime
- Wetsartikel
- Video
- Handig

INDEX

Politie en OM nog te weinig bezig met internetcriminaliteit

Politie en justitie besteden steeds meer aandacht aan het opsporen en vervolgen van internetcriminelen, maar nog niet zoveel als was afgesproken.
Het OM behandelde vorig jaar 171 cybercrimezaken, bijna vijftig meer dan een jaar eerder, staat in het jaarrapport van het Openbaar Ministerie.
Afgesproken was dat het OM 190 zaken op het gebied van internetcriminaliteit zou behandelen, dus de norm is niet gehaald. "Dat heeft te maken met het feit dat de politie en OM nog bezig zijn met een noodzakelijke inhaalslag op het vlak van expertise en capaciteit op dit terrein", concludeert het Openbaar Ministerie.

Achterstand
Het is al langer bekend dat de politie een achterstand heeft weg te werken. Er zijn speciale cyberteams opgericht en de politie probeert onder meer met een online game rechercheurs te werven.
In het jaarrapport worden ook enkele successen genoemd. Zo staat staat het OM stil bij een zaak waarin criminelen tienduizenden versleutelde Blackberry's verkochten. Het dataverkeer was voor justitie onzichtbaar doordat gebruik gemaakt werd van eigen computerservers in Nederland en Canada, die alle communicatie versleutelden. Ook waren vaak de microfoon en camera uit het toestel gehaald, zodat niemand ze kon afluisteren.
Het OM kwam de telefoons op het spoor, doordat bij liquidatiezaken opvallend vaak telefoons met versleuteling gevonden werden. Uiteindelijk werd het netwerk in april vorig jaar door het OM offline gehaald.

Bewijsmateriaal
Op de servers staan 3,6 miljoen versleutelde berichten uit de georganiseerde misdaad, zegt het OM. "Met het ontsleutelen van de informatie komt bewijsmateriaal beschikbaar voor tientallen strafrechtelijke onderzoeken naar liquidaties, gewapende overvallen, drugshandel, witwassen, pogingen tot moord en andere georganiseerde criminaliteit."
Ook gaat het OM in op een internationaal onderzoek uit november naar een botnet met servers in Nederland, waarbij 500.000 computers offline zijn gehaald. In totaal zijn in 30 landen acties uitgevoerd en zijn vijf verdachten opgepakt.
Scheidend OM-voorzitter Bolhaar complimenteert zijn collega's in het jaarrapport. "Het afgelopen jaar is met talloze strafzaken bijgedragen aan een rechtvaardiger en veiliger Nederland. De medewerkers van het OM verdienen een groot compliment voor hun grote betrokkenheid en vakmanschap."

Bron: HCC

INDEX

Rechtspraak heeft meer kennis van cybercrime nodig

De Rechtspraak heeft meer kennis van cybercrime nodig, alsmede financiële investeringen, om deze vorm van criminaliteit het hoofd te kunnen bieden. Dat liet Leendert Verheij, president van het gerechtshof Den Haag, tijdens de jaarlijkse themadag van het Kenniscentrum Cybercrime van de Rechtspraak weten. Volgens Verheij is er op het gebied van cybercrime sprake van een toenemende omvang.
Dit vereist investeringen in geld, kennisverwerving, kennisontwikkeling en kennisdeling aan de kant van de Rechtspraak, merkte hij op. Het Kenniscentrum Cybercrime, verbonden aan het gerechtshof Den Haag, houdt zich met het kennisgedeelte bezig. Zo zijn er wiki's, worden er cursussen gegeven en themadagen georganiseerd. Volgens Verheij zijn dit soort initiatieven hard nodig, want cyberzaken worden technisch en juridisch steeds complexer.

"Dit heeft te maken met de toenemende complexiteit van het digitaal forensisch onderzoek en de even-eens toenemende schaal en "sophistication" van de onderliggende criminele activiteiten. Daarbij speelt tevens een rol dat de politie nog zeer zoekende is in de manier waarop daarover het beste kan worden geverbaliseerd.
Dit leidt niet zelden tot het stellen van nadere vragen aan (een) deskundige(n), en levert in die zin dus ook een groter beslag op zittingstijd op", aldus de president van het gerechtshof Den Haag.

Deze ontwikkeling zal volgens Verheij alleen maar doorzetten, waarbij er een steeds groter beroep wordt gedaan op ook het ict-technische kennis- en begripsniveau van de behandelend rechters. "Het is in dit licht dan ook opvallend dat het Kenniscentrum bemerkt dat de animo van collega's voor cursussen en presentaties soms tegenvalt, en daarnaast dat het kennisniveau van een groot deel van onze collega's het minimale niet overstijgt of zelfs niet bereikt", liet Verheij weten.

Binnen de Rechtspraak is een projectplan gestart om kennis te delen, maar volgens Verheij is het veel belangrijker dat de belang-stelling voor de materie en de vraag naar verdere ontwikkeling van cybercrimekennis vanuit de professionals zelf komt. "We zullen vooral aandacht vragen voor de verantwoor-delijkheid van professionals om te investeren in uitbreiding van kennis en het opdoen van ervaring op dit terrein, waarvan we immers één ding zeker weten: het gaat om een 'groeimarkt' en zeker niet om een verschijnsel dat zal wegebben."

INDEX

Nederland kwetsbaar voor ransomware

Van alle aanvallen met ransomware in Europa is 3,4 procent gericht tegen Nederlanders. Italië is doelwit van ruim 7 procent van de gijzelsoftware en Rusland 3 procent. Wereldwijd staat Nederland op plek zes.

Talenknobbel
Volgens expert Dick O'Brien van Symantec is het hogere aantal aanvallen in Nederland mogelijk te verklaren door het feit dat Nederlanders goed Engels spreken. De meeste e-mails met ransomware zijn opgesteld in het Engels en door de Nederlandse talenknobbel zijn mensen eerder geneigd om bijvoorbeeld links of bestanden in e-mails met ransomware aan te klikken.
Diefstal
Nederlanders worden ook relatief vaak getroffen door diefstal van een online-identiteit. Wereldwijd staat Nederland op plek negen. In 2016 werden bijna 6,6 miljoen online-identiteiten gestolen. Het gaat dan bijvoorbeeld om de inloggegevens voor e-mail, maar ook complete persoonsgegevens. Op de eerste plek in de lijst staan de Verenigde Staten. De tweede plek wordt ingenomen door Frankrijk.

Cyberaanvallen uit Nederland
Opvallend in het rapport is verder dat Nederland ook hoog genoteerd staat wat betreft de oorsprong van cyberaanvallen. In totaal komt 1,8 procent van alle computeraanvallen uit Nederland.
Daarmee is Nederland zesde wereldwijd; in 2015 voerde Nederland deze ranglijst nog aan. Waarom Nederland minder aantrekkelijk is geworden als basis om aanvallen te lanceren is niet duidelijk. Het kan zijn dat de kosten voor aanvallen vanuit Nederland zijn gestegen, maar ook dat de politie meer aandacht besteedt aan cyberaanvallen.

Bron: Telegraaf

INDEX

50 procent meer ransomware-aanvallen in 2016

Het aantal ransomware-aanvallen neemt toe, en klassieke technieken zoals social engineering en voorspelbare wachtwoorden geven cybercriminelen vrij spel.

Organisaties blijven het cybercriminelen makkelijk maken om hun slag te slaan. Dat blijkt uit het jaarlijkse security-onderzoek van Verizon. In hun Data Breach Investigations-rapport werden ruim 40.000 security-incidenten en bijna 2.000 datalekken geanalyseerd die gedurende het afgelopen jaar plaatsvonden. Uit de resultaten blijkt dat de gemiddelde cyberincident wordt gepleegd door een externe partij, zoals een of meerdere cybercriminelen, en plaatsvindt met behulp van een hack.

Bovendien blijkt ook dat niet enkel grote organisaties worden geviseerd: 61 procent van de slachtoffers waren bedrijven met minder dan duizend werknemers. Bij meer dan de helft van alle aanvallen werd daarnaast gebruikt gemaakt van malware, zoals ransomware of spyware

Meer ransomware

Vooral ransomware kent een opmars: in 2016 werden 51 procent meer ransomware-aanvallen opgetekend dan het jaar daarvoor. Desondanks lijkt het aantal tegen het einde van 2016 weer af te nemen. In het laatste kwartaal daalde de hoeveelheid aanvallen met maar liefst 70 procent, onder meer door de teloorgang van populaire ransomware-vormen Locky en CryptoWall. Het rapport verwijst bovendien naar initiatieven zoals No More Ransom, waarvan ook België sinds kort deel uitmaakt, die de verspreiding van ransomware tegengaan.

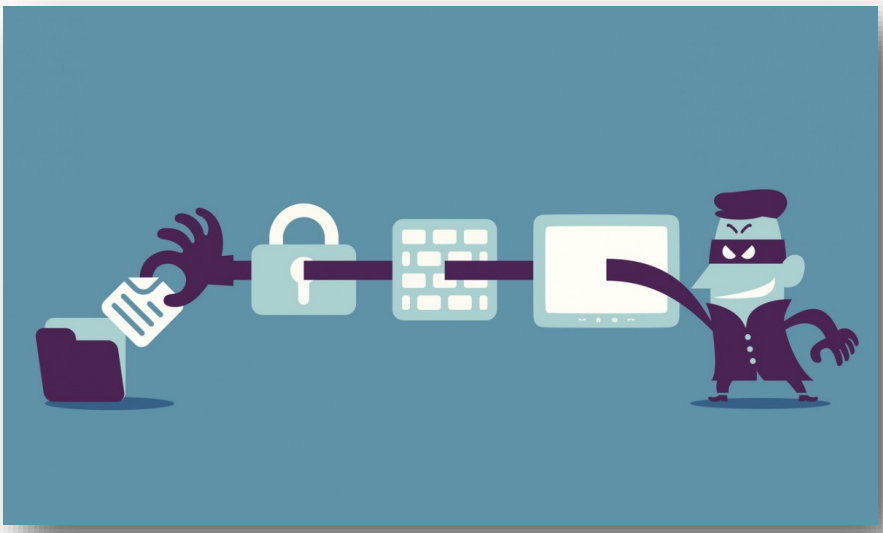
Phishing en wachtwoorden

Hoewel cybercriminelen hun wapens licht aanpassen, blijft de methode van infiltratie nagenoeg hetzelfde. Zo'n 88 procent van alle cyberaanvallen kan worden ondergebracht in negen categorieën die Verizon in 2014 al vastlegde, waaronder crimeware, denial of service en cyberspionage. Social engineering wordt ingezet bij meer dan 90 procent van alle security-incidenten, waarbij phishing en pretexting het vaakst worden aangewend. Werknemers blijken dan ook gevoelig voor zulke pogingen. Zo'n 7 procent klikte op een verdachte link of bijlage in een phishingmail, en een kwart daarvan deed dat ook een tweede keer. Zodra het slachtoffer de webpagina of bijlage opent, wordt er in 95 procent van de gevallen malware gedownload om data te stelen of de controle over systemen over te nemen.

Ook het wachtwoordgebruik blijkt nauwelijks verbeterd te zijn. Werknemers gebruiken nog steeds zwakke wachtwoorden die bijvoorbeeld makkelijk te kraken zijn of hetzelfde wachtwoord voor meerdere accounts. Cybercriminelen maken daar handig gebruik van, aangezien 80 procent van de security-lekken die via een hack gebeurde, mogelijk werd gemaakt door een gestolen en/of zwak wachtwoord.

Menselijke fouten

Het rapport concludeert dat bedrijven kwetsbaar blijven voor de klassieke aanvalstechnieken, ook al zijn die al jaren onveranderd. Volgens Bryan Sartin, executive director bij Verizon Enterprise Solutions, heeft dat te maken met enkele menselijke eigenschappen. "Cybercriminelen concentreren zich op vier belangrijke vormen van menselijk gedrag om medewerkers aan te moedigen informatie prijs te geven: gretigheid, afleiding, nieuwsgierigheid en onzekerheid," zegt Sartin. "En zoals uit ons rapport valt op te maken, blijkt dit te werken."



In het rapport worden tot slot nog enkele tips meegegeven om de impact van cyberincidenten te beperken. Zo is het belangrijk om altijd zo snel mogelijk updates en patches uit te voeren, gevoelige data te versleutelen en tweefactor-authenticatie in te schakelen bij het inloggen. Bovendien wordt aangeraden om van werknemers de "eerste verdedigingslinie" te maken: train gebruikers in het herkennen van verdachte e-mails, en maak het mogelijk om zo'n incidenten te rapporteren.

Bron: Verizon

INDEX

Wat is Wannacry en wat is er gebeurd?

'Oeps, uw bestanden zijn versleuteld! Foto's, bestanden, databanken, en andere gegevens zijn onbereikbaar. U kunt de bestanden weer vrij krijgen, maar u heeft daarvoor niet zo genoeg tijd', zo luidde de boodschap. Wat is Wannacry en waar komt het vandaan?

Wannacry is ransomware die een (recent gepatcht) lek in Microsoft Windows gebruikt om zich razendsnel te verspreiden via interne netwerken. Om precies te zijn maakt de ranwsomware gebruik van een lek in Windows SMB Server. Overigens heeft Microsoft al op 14 maart een patch hiervoor uitgebracht.
De ransomware lijkt te worden verspreid via een massale mailingcampagne. Zodra een machine is geïnfecteerd, scant die het interne netwerk om collega's aan te steken. Die machines hoeven daarvoor niet zelf met het internet verbonden zijn.
De exploit die Wannacry gebruikt, Eternalblue SMB, was een van de tools die in april gelekt werden door hakingroep TheShadowBrokers. Die maakten ze dan weer buit bij de Amerikaanse inlichtingendienst NSA. De SMB-exploit, en de ransomware die hem gebruikt, werkt op alle versies van Windows die nog niet gepatcht zijn met de update MS17-010, die Microsoft op 14 maart uitbracht. Windows 10 en Windows Server 2016 zijn wel standaard beschermd tegen het lek.

Dat Wannacry niet nog meer slachtoffers maakte, is te danken aan een securityonderzoeker van de blog MalwareTech, en een hele hoop toeval. De malware in kwestie is namelijk uitgerust met een hardcoded 'kill switch' of noodrem die de hele boel kan stilleggen. Wannacry probeert tijdens zijn proces verbinding te maken met een webdmein, www.iuqerfsodp9ifjaposdfjhgosurijfaewrwergwea.com. Als die verbinding lukt, stopt het encryptieproces. De onderzoeker kwam tot de vaststelling dat die domeinnaam niet door de hackers was geregistreerd en kon voor zo'n elf dollar de domeinnaam zelf kopen. Na de registratie ervan volgden duizenden verbindingen per seconde. Het is dus voor beheerders van computernetwerken zaak om dat domein vooral niet te blokkeren.
Securityfirma Fox-IT merkt fijntjes op dat dit een slordige vergissing is van de hackers, gezien de grootte van hun malwarecampagne. Iedereen die de phishingmail kreeg en hem pas opende nadat MalwareTech het domein openstelde, is dus van de meeste miserie bespaard gebleven. De deskundige, die twittert onder de naam MalwareTech, verduidelijkt in een tweetbericht overigens dat hij aanvankelijk geen idee had welke gevolgen het registreren van de domeinnaam zou hebben. Het afblokken van de woekerende cyberaanval gebeurde dus eigenlijk toevallig, laat hij blijken. De 'killswitch' heeft geen invloed op computers die al besmet waren.

Gezien de ransomware exploits gebruikt in verouderde versies van Windows, adviseert Microsoft gebruikers van Windows 7 en Windows XP alvast om zo snel mogelijk hun systeem te updaten. Het bedrijf heeft een patch uitgebracht voor Windows 7, genaamd MS17-010 die het lek moet dichten, ook voor Windows XP zijn er updates. Fox-IT, dat een rapport opstelde over de ransomware, raadt gebruikers en beheerders ook aan om het SMBv1 protocol uit te zetten, en RDP- en SMB connecties van het internet te blokkeren. Toestellen die niet geüpdatet zijn, kun je best van het internet halen (en van het interne netwerk) en zoals altijd met ransomware: zorg dat je goede back-ups hebt van je belangrijke gegevens.
Goed om weten is trouwens dat er een registry key in de ransomware zit, die ervoor zorgt dat de malware niet zomaar kan worden tegengehouden met een reboot. Het is dus echt wel zaak om te updaten.

De cyberaanval heeft intussen al wel zo'n 200.000 slachtoffers gemaakt in tenminste 150 landen. Onder meer Britse ziekenhuizen, de Russische overheid, de Duitse spoorwegen en Franse fabrieken van autobouwer Renault werden getroffen alsmede verschillende parkeergarages van Q-Park in Nederland. In België is de schade tot dusverre ook beperkt gevleven. Het Centrum voor Cyberveiligheid (CCB) daar meldde rond zaterdagmiddag één mogelijk slachtoffer.
"We voeren jaarlijks tegen zowat tweehonderd cyberaanvallen operaties uit, maar hebben nog nooit zoiets meegemaakt als dit", zegt Rob Wainwright van Europol daarover.
De aanval mikte vooral op bedrijven, wat consistent is met het 'zakenmodel' van ransomware. Bedrijven hebben vaker belangrijke gegevens, en ze hebben ook meer geld om hackers te betalen. Computers die gegijzeld werden door de ransomware werden voor 300 dollar in bitcoins (ongeveer 275 euro) weer vrijgegeven.

De Wannacry ransomware maakt gebruik van een lek in het besturingssysteem SMB Server en het werd oorspronkelijk ontwikkeld door de Amerikaanse inlichtingendienst NSA. Die hield kennis over het lek met andere woorden voor zich, om het achterpoortje te kunnen gebruiken. De ransomware werd echter zelf buitgemaakt door hackers.
Voor Microsoft-voorzitter Brad Smith is het alvast welletjes geweest. "Deze aanval is een nieuw voorbeeld van waarom de opslag van gevoeligheden door de overheden zo'n groot probleem is", schrijft hij in een blogpost. "'Dit is een patroon dat steeds vaker voorkomt in 2017. Exploitaties in de handen van overheden zijn al vaker gelekt geweest naar het publieke domein en zo grote schade veroorzaakt", aldus Smith.

INDEX

Europese Unie wil sociale media aanmanen zelf haatberichten op te sporen

Europa wil een eenduidige strategie ontwikkelen voor de aanpak van haatberichten, kindermishandeling, terrorisme en andere illegale content op sociale media. Momenteel verschilt de aanpak van land tot land en dienst tot dienst. Overkoepelende wetgeving moet de strijd tegen illegale posts een duidelijk kader geven. Dat weet Reuters, dat een vroege versie van een beleidsnota van de Europese Commissie kon inkijken.

Die maakt zich zorgen om de grote verscheidenheid in strategieën tegenover de verwijdering van illegale content. Soms kan dat geen kwaad, maar in de praktijk merkt de commissie een te trage responstijd wanneer het er volgens haar echt toe doet, bijvoorbeeld bij het aanzetten tot terrorisme, kinderporno of copyrightschendingen. De individuele aanpak van landen kan bovendien te veel naar de andere kant van het spectrum doorslaan. Zo introduceerde Duitsland vorige maand wetgeving waarbij het land sociale mediadiensten een boete van 50 miljoen euro kan opleggen wanneer ze haatposts niet snel genoeg verwijderen.

Spreidstand
Sociale media zoals Facebook, Google en Twitter zijn langs de ene kant niet verantwoordelijk voor de onzin die jij en ik online plaatsen. Langs de andere kant is het wel hun job om schadelijke berichten te verwijderen. Die spreidstand zorgt al te vaak voor een te trage reactie van de diensten zelf.
De Europese Commissie denkt aan de implementatie van het principe van de goede Samaritaan. Daarbij moeten sociale mediaproviders zelf op zoek gaan naar posts die indruisen tegen de Europese wetgeving maar zonder resultaatverbintenis. Een duidelijk actief engagement om dergelijke berichten op te sporen is dan verplicht, maar wanneer er toch één door de mazen van het net glipt, kijkt een dienst niet meteen tegen monsterboetes aan. Het aanmoedigen van een proactieve aanpak van de diensten moet het probleem deels verhelpen zonder dat Facebook of Twitter bang moeten zijn voor zware represailles wanneer iemand hun diensten toch misbruikt.

YouTube, Microsoft, Facebook en Twitter maakten eerder al het engagement om binnen de 24 uur tegemoet te komen aan de vraag om content te verwijderen afkomstig van een overheid, maar de commissie vindt dat er nog werk aan de winkel is.

INDEX

Windows-hackingtools van NSA gelekt: is jouw pc besmet?

Het hackerscollectief de Shadowbrokers heeft de voorbije maand verschillende bestanden gelekt die afkomstig zouden zijn van de National Security Agency (NSA) van de Verenigde Staten. In de recentste documenten zitten exploits voor verschillende versies van Windows (Server) die door Hacker Fantastic worden beschreven als een “Microsoft-apocalyps”. Beveiligingsspecialisten zeggen dat de exploits goed geschreven zijn en vermoeden dat cybercriminelen de gelekte tools eveneens gebruiken. Uit onderzoek blijkt dat zo’n honderdduizend pc’s besmet zijn via de exploits.

Doublepulsar
Veel van de exploits die in de gelekte documenten worden beschreven, maken gebruik van dezelfde payload, Doublepulsar genaamd. Deze payload dringt binnen in de kernel van een systeem en wordt gebruikt om willekeurige dll’s te injecteren. Cybercriminelen en de NSA kunnen hierdoor computers besmetten met malware, waarna ze de eigenaar van de besmette pc kunnen bespioneren.

BinaryEdge ontwikkelde een script waarmee het computers detecteert waarop Doublepulsar aanwezig is. Op 23 april telde de beveiligingsspecialist maar liefst 164.715 geïnfecteerde computers, wat zelfs voor de NSA een erg groot aantal is. Hoogstwaarschijnlijk hebben cybercriminelen de gelekte gegevens van de Shadowbrokers gebruikt om zelf met de hackingtools aan de slag te gaan. Gebruikers die hun pc niet van de recentste patches hebben voorzien, lopen hierdoor groot risico om malware op te lopen.

In zijn blogpost deelt BinaryEdge een top tien van landen met de meeste pc’s die getroffen zijn door de hackingtools. De Verenigde Staten prijkt met grote marge op nummer een, met maar liefst 67.052 besmette computers. Ook Nederland vind je terug in de lijst, met 1.479 besmettingen. In België zijn er daarentegen slechts 117 pc’s geïnfecteerd.

Bron: Shadowbrokers

INDEX

Nederland in top 10 identiteitsdiefstal

Nederland staat op plek 9. In 2016 werden bijna 6,6 miljoen online identiteiten gestolen. Het gaat dan bijvoorbeeld om de inloggegevens voor e-mail, maar ook complete persoonsgegevens. Op de eerste plek in de lijst staan de Verenigde Staten. De tweede plek wordt ingenomen door Frankrijk.

Opvallend is dat het in 2016 vooral ging om een aantal grootschalige gevallen van diefstal. Zo werden in Frankrijk ruim 85 miljoen online identiteiten buitgemaakt na een lek bij videosite Dailymotion. In Rusland werden bij twee diefstallen meer dan 83 miljoen identiteiten gekaapt.

Tweede Boek. Misdrijven

Titel XII. Valsheid met geschriften, gegevens en biometrische kenmerken

Artikel 231b Hij die opzettelijk en wederrechtelijk identificerende persoonsgegevens, niet zijnde biometrische persoonsgegevens, van een ander gebruikt met het oogmerk om zijn identiteit te verhelen of de identiteit van de ander te verhelen of misbruiken, waardoor uit dat gebruik enig nadeel kan ontstaan, wordt gestraft met een gevangenisstraf van ten hoogste vijf jaren of geldboete van de vijfde categorie.

INDEX

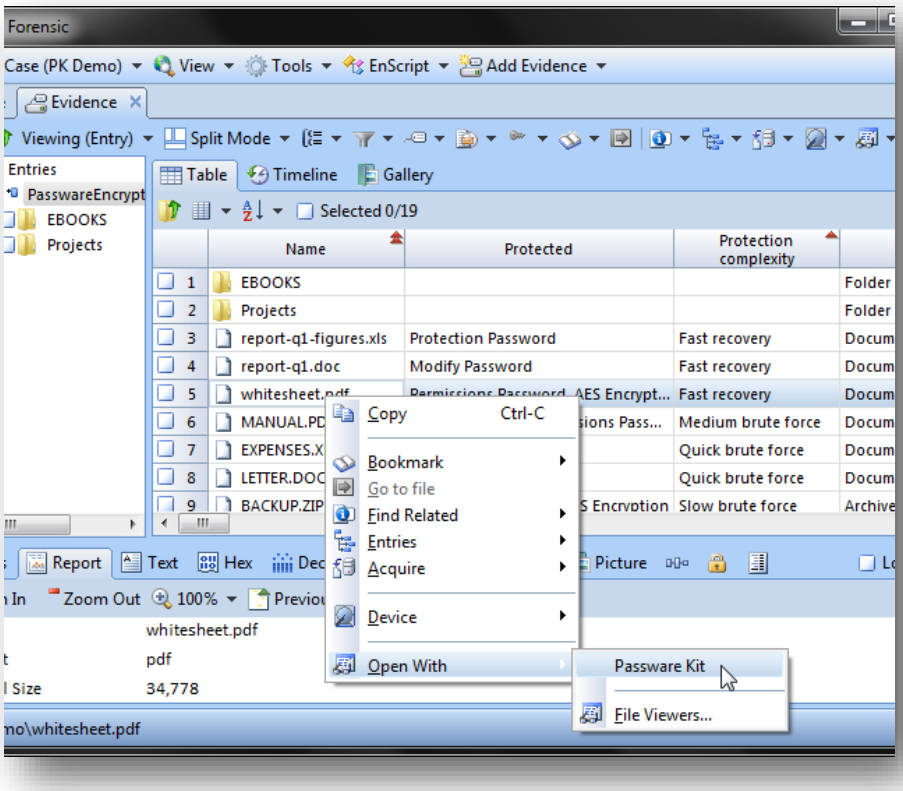
Forensische tool politiediensten bevat beveiligingslek

Een tool die opsporings- en politiediensten wereldwijd gebruiken voor het veiligstellen van digitaal bewijs bevat een kwetsbaarheid waardoor een aanvaller het systeem van de forensisch onderzoeker kan overnemen en de ontwikkelaar van de software is niet van plan om een beveiligingsupdate uit te brengen. De kwetsbaarheid bevindt zich in de EnCase Forensic Imager. Een gratis tool waarmee een forensisch onderzoeker bewijsmateriaal van opslagmedia kan veiligstellen. Het bewijsmateriaal is vervolgens later in de commerciële EnCase Forensic suite te analyseren. Onderzoekers van beveiligingsbedrijf SEC Consult ontdekten een beveiligingslek in de Forensic Imager. Door een opslagapparaat te voorzien van een geprepareerde LVM2-partitie is het mogelijk om het systeem van een forensisch onderzoeker over te nemen als die het apparaat onderzoekt.

Het kan dan bijvoorbeeld gaan om een usb-stick van een verdachte die wordt onderzocht, waarbij de onderzoeker via de Forensic Imager de datadrager onderzoekt. Via de kwetsbaarheid kan een aanvaller de machine van de onderzoeker verbinding met bijvoorbeeld zijn server laten maken. Vervolgens is het mogelijk om bewijs op de machine van de onderzoeker te manipuleren of te verwijderen, aldus de onderzoekers. De producten van Guidance Software, ontwikkelaar van EnCase, worden onder andere door de FBI, CIA, NAVO en de Nederlandse Politieacademie gebruikt, alsmede grote bedrijven zoals Microsoft, Facebook, Apple en Yahoo.

Volgens de onderzoekers maken sommige organisaties gebruik van speciale machines zonder netwerk- of internettoegang om met bewijsmateriaal om te gaan, maar zou dat niet tegen deze aanval beschermen. Een aanvaller kan nog steeds malware maken die bewijsmateriaal verwijdert. Zo kan de malware bijvoorbeeld alle Excel-bestanden op het systeem verwijderen of bestanden waarin een bepaalde naam voorkomt.

SEC Consult waarschuwde Guidance Software in maart van dit jaar, maar het bedrijf heeft geen oplossing uitgebracht en is dit ook niet van plan. Volgens het softwarebedrijf gaat het om een randgeval en komt er bij het verwerken van "raw data" altijd een risico kijken. Guidance Software stelt verder dat het niet om een ernstig probleem gaat. In onderstaande video wordt de kwetsbaarheid gedemonstreerd.



INDEX

AI-systeem Watson wordt wapen in de strijd tegen cybercriminaliteit

IBM's Watson is klaar om het tegen cybercriminelen op te nemen. Het systeem krijgt een grote rol binnen IBM's security-platform, en wordt binnenkort ook beschikbaar als virtueel assistent.

Een jaar lang werd IBM's Watson getraind in de "taal van cybersecurity", waarbij het artificieel intelligente systeem meer dan één miljoen documenten bestudeerde. Nu die trainingsperiode afgelopen is, wordt Watson in de praktijk ingezet om security-wetenschappers bij te staan in de strijd tegen cybercriminaliteit.

Mens en machine

IBM plant om Watson te integreren in meerdere facetten van hun security-aanbod. Het AI-systeem krijgt zo een centrale plaats in IBM's nieuwe 'security operations center'-platform, oftewel het Cognitive SOC-platform, dat ingezet kan worden om dreigingen rond pc's, netwerk en cloudsoftware op te sporen. Zo zoekt IBM een oplossing voor de rijzende cyberdreiging, verklaart Denis Kennelly, vicepresident binnen IBM Security. "Het Cognitive SOC is nu een realiteit voor klanten die een wapen zoeken tegen de toenemende massa aan cybercriminelen en next-gen dreigingen," meent Kennely. "Het combineren van de unieke capaciteiten van mens en intelligente machine is cruciaal voor het volgende stadium in het gevecht tegen geavanceerde cybercriminaliteit."

Van weken naar uren

De eerste tool die gebruik zal maken van Watsons redeneervermogen is IBM's QRadar Advisor, een app voor security-analisten. Om te weten of een incident effectief een gevaar vormt voor het bedrijf, moeten security-analisten zo'n dreiging beoordelen door bijvoorbeeld blogs, security-bulletins en live threat-feeds te bestuderen. Het is een tijdsintensieve klus, waarbij altijd de kans bestaat dat bronnen over het hoofd worden gezien of dreigingen fout worden geïnterpreteerd. Door artificiële intelligentie in te zetten, kan het hele proces echter aanzienlijk worden ingekort, schrijft IBM.

Zo is Watson in staat om al die bronnen veel sneller door te nemen, omdat het systeem getraind is om natuurlijke taal te interpreteren. De beschikbare informatie – van online bronnen tot IBM's eigen data – worden door Watson bestudeerd, waarna hij de relevante bronnen kan selecteren die nuttig kunnen zijn in het onderzoek. De analist blijft dus essentieel in het gebeuren, maar het uiteindelijke proces kan versneld worden tot slechts enkele uren of minuten, beweert IBM.

Virtuele assistent

Daarnaast maakt het bedrijf bekend dat het werkt aan een virtuele assistent op basis van Watson. De assistent krijgt de naam Havyn en reageert op stemcommando's, zoals Siri of Alexa. Havyn moet fungeren als een security-assistent die analisten kunnen raadplegen om realtime informatie te krijgen, bijvoorbeeld bij een urgente cyberdreiging, en doet voor de antwoorden een beroep op vrij beschikbare informatie online, maar ook op bedrijfsspecifieke data. De assistent wordt op dit moment uitgebreid getest binnen IBM.

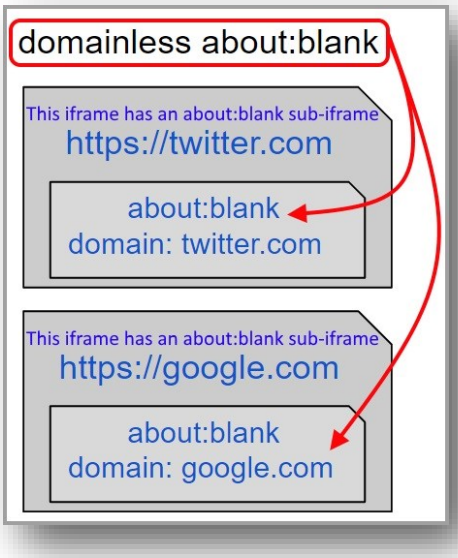
Ten slotte kunnen bepaalde klanten zich al wenden tot een chatbot die gebaseerd is op Watson. De bot werkt niet met stemcommando's, maar kan wel geraadpleegd worden met vragen over netwerkconfiguraties, security-status, en technische ondersteuning.

Bron: SmartBiz

INDEX

Microsoft Edge gooit je paswoorden te grabbel

Via een lek kunnen hackers alle logingegevens die Edge bewaart van je ontvreemden. Hierdoor kunnen hackers onder andere tweeten in jouw naam.



Beveiligingsspecialisten zijn een kwetsbaarheid in Edge op het spoor gekomen die ervoor zorgt dat hackers je logingegevens kunnen stelen. Eenmaal je een kwaadaardige link hebt aangeklikt, kan een cybercrimineel al je cookies verzamelen. Tot deze cookies behoren de logingegevens die door de standaard wachtwoordmanager van Edge worden bewaard. De hacker vergaart voldoende informatie om onder andere je Twitter-account over te nemen. Zelfs wanneer je het sociale medium in een ander venster dan de malware geopend hebt, kunnen hackers in jouw naam berichten plaatsen.

Same origin policy

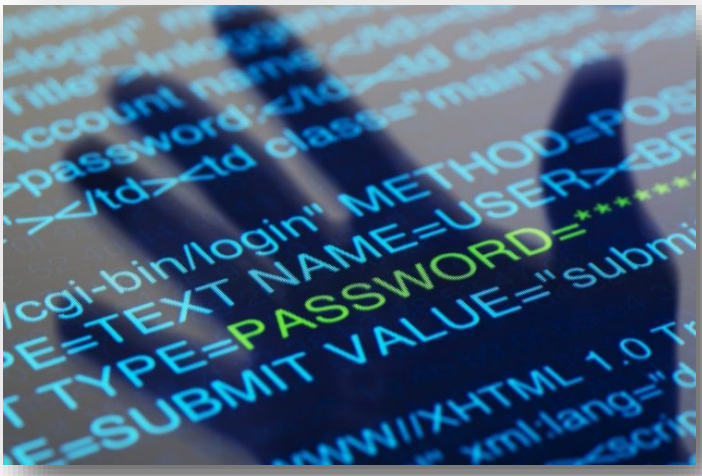
Aan de basis van het probleem ligt de 'same origin policy' (SOP) van Edge. SOP wordt in alle moderne browsers gebruikt om te voorkomen dat pagina's zonder een domein andere pagina's kunnen wijzigen. Normaal gezien krijgen about:blank-pagina's steeds het domein van hun verwijzer. Een about:blank van een iframe in Twitter kan hierdoor niet aan een about:blank van Google.
In het verleden was het in Edge echter mogelijk om about:blanks te creëren zonder een domein. Deze pagina-elementen kunnen alle about:blanks raadplegen, ongeacht tot welk domein deze behoren.
Iframes van onder andere Twitter en Google bevatten about:blanks, welke met behulp van een zelf gecreëerde about:blank geraadpleegd konden worden, met alle gevolgen van dien.
Microsoft dichtte het lek door ervoor te zorgen dat about:blanks steeds een domein hebben. Wanneer je een dergelijke pagina opent, krijgt deze een willekeurig nummer toegekend dat fungeert als het domein. Iedere about:blank die je zelf creëert, heeft een uniek domein, waardoor interactie tussen de pagina-elementen onmogelijk is.

Hack

Beveiligingsspecialisten van Broken Browser zijn een manier op het spoor gekomen om de nieuwe beveiliging in Edge te omzeilen. Via een omweg kan je nog steeds een about:blank zonder domein creëren, wat de start vormt van een interessante hack. In een filmpje laat Broken Browser zien hoe het de logingegevens van Charles Darwin steelt en vervolgens in zijn naam berichten tweet.
In het filmpje begint de hack op het moment dat Darwin een kwaadaardige link aanklikt. De malware die hierdoor wordt gestart, kan de cookies van de man ontvreemden. Hierna is het kinderspel om de logins van Darwin te vergaren en zijn accounts over te nemen.

Onveilige Edge

Microsoft creëerde Edge vanaf nul om een veiligere browser dan Internet Explorer aan te bieden. Uit deze hack blijkt jammer genoeg wederom dat ook Edge niet vrij van fouten is. Ook tijdens het hackersevent Pwn20wn 2017 viel de browser door de mand. Tijdens dit event proberen hackers zo snel mogelijk exploits in browsers te vinden. Chrome werd dit jaar niet gehackt, terwijl de experts maar liefst vijf kwetsbaarheden in Edge vonden op twee dagen tijd. Hierdoor ging de browser met de titel lopen van meest gehackte browser.



INDEX

Nieuwe richtlijnen moeten wachtwoordgebruik hervormen

Het National Institute of Standards en Technology stelde een nieuwe set regels op die wachtwoordbeveiliging moet verbeteren. Enkele aanpassingen gaan lijnrecht tegen in de huidige standaarden in.

Wachtwoorden zijn de meest voorkomende manier om data te beschermen: ze zijn makkelijk te implementeren en kosten geen geld. Ideaal is de methode echter niet. Vele gebruikers kiezen voor te eenvoudige combinaties, waardoor de wachtwoorden kunnen worden gekraakt. Het NIST stelt daarom geregeld aanbevelingen voor die het wachtwoordgebruik kan verbeteren. In het laatste document stelt de organisatie drie opvallende aanpassingen voor, die voor het eerst gemeld werden door VentureBeat.

Niet meer verplicht aanpassen

Gebruikers zouden niet meer gevraagd mogen worden om hun wachtwoord om de zoveel tijd aan te passen. Beter nog: een wachtwoord zou enkel aangepast mogen worden indien de gebruiker dat zelf wilt of als er bewijs is dat het wachtwoord niet meer veilig is, bijvoorbeeld na een hack. Als gebruikers verplicht worden om hun wachtwoord periodiek te veranderen, kiezen ze immers vaak voor variaties op hetzelfde wachtwoord in een voorspelbaar patroon. Zelfs wanneer je elke maand je wachtwoord aanpast, ben je er nog niets mee indien dat wachtwoord voorspelbaar is.

Geen inhoudelijke regels

Bijna elke website of online service stelt regels aan de wachtwoorden van hun gebruikers, zoals “minimum acht tekens, één symbool en één cijfer”. De achterliggende gedachte is logisch, maar ook hier kan de regel net het omgekeerde effect hebben. Gebruikers die gedwongen worden om hun wachtwoord zo ‘speciaal’ mogelijk te maken, zullen niet per se een sterk wachtwoord gebruiken maar in de plaats daarvan bestaande woorden licht aanpassen. Zo komen we aan klassiekers als ‘w@chtwoord1’. De regel creëert een vals gevoel van veiligheid, en kan dus beter achterwege worden gelaten.

Altijd vergelijken

Wat online verifieerders wél moeten doen, is controleren of de gekozen wachtwoorden voldoen aan de vereisten van een sterk wachtwoord. Nieuwe combinaties zouden vergeleken moeten worden met een lijst van voorspelbare wachtwoorden, waaronder:

- bestaande woorden;
- wachtwoorden die eerder gestolen werden;
- repetitieve of opeenvolgende tekens, zoals: ‘11111’ of ‘ABC123’;
- contextspecifieke woorden, zoals de naam van de website of de gebruikersnaam.

De aanbevelingen van het NIST zijn niet verplicht, maar worden gevolgd als leidraad door securityprofessionals en websitebeheerders. Met de nieuwe regels zouden velen onder hen de huidige standaarden moeten aanpassen. Overigens werden ook andere verificatiemethodes in het document behandeld, zoals biometrische methodes of OTP-toestellen, maar daarbij werden geen opvallende veranderingen vastgesteld.

INDEX

Inlichtingendiensten wissen gegevens niet

De CTIVD nam alle hacks onder de loep die de diensten tussen 1 januari 2015 en 17 maart 2016 uitvoerden. De commissie concludeert dat de AIVD en MIVD ,,doorgaans weloverwogen te werk gaan'', maar ze somt ook de manieren op waarop de inlichtingendiensten in strijd met de regels handelen.

Een daarvan is het niet-wissen van gegevens hoewel dit volgens de regels wel zou moeten. Daarnaast hanteren de diensten nog steeds geen bewaartermijnen voor gegevens die nog moeten worden geëvalueerd, hoewel hier eerder wel toezeggingen over zijn gedaan aan de Tweede Kamer. ,,Hiermee handelen de diensten onrechtmatig'', concludeert de commissie. Ze raadt een maximale bewaartermijn van een jaar aan voor ongeëvalueerde gegevens.

De AIVD heeft een aantal keer operaties uitgebreid zonder daar opnieuw toestemming voor te vragen. ,,Een voorbeeld daarvan was een operatie waarbij op een toestemming voor het hacken van een laptop een daarvan losstaand internetaccount van hetzelfde target werd bijgeschreven'', schrijft de commissie. Vaak werd na afloop door de minister wel toestemming gegeven voor de uitbreiding, maar dat gebeurde pas nadat de diensten al in hun doelwit waren binnengedrongen.

Voor hacks op afstand moeten beide diensten de verantwoordelijke minister om toestemming vragen. Bij fysieke hacks, zoals een in beslag genomen computer, is bij de AIVD toestemming van de directeur van de dienst nu nog voldoende. De redenering daarvoor - dat een fysieke hack tijdelijker van aard is en daardoor een minder ernstige inbreuk op privacy - vindt de CTIVD allesbehalve overtuigend. De commissie adviseert daarom om ook voor fysieke hacks toestemming van de minister verplicht te stellen.

De commissie gaat ook in op het gebruik door de diensten van kwetsbaarheden in digitale beveiliging. De CTIVD wijst vooral op het belang van kwetsbaarheden die nog niet algemeen bekend zijn bij gebruikers of softwareontwikkelaars: de zogenoemde zero days. De diensten hebben geen regels om dit soort lacunes aan te kaarten bij ontwikkelaars, ook niet als het beveiligingslek niet meer hoeft te worden stilgehouden voor het onderzoek. Hier moet verandering in komen, vindt de CTIVD.

Bron: CTIVD

INDEX

Meer slachtoffers en schade door 'Microsoft-helpdesk'

Fraudeurs die zich voordoen als Microsoft-helpdesk scoren grotere geldbedragen bij meer slachtoffers in Nederland. Begin 2017 overtreft begin 2016 en de schade nadert al het totaal van 2017.
De aloude oplichtingspraktijk van telefonische scammers zit in de lift. De fraudeurs die mensen bellen en zich voordoen als "de Microsoft-helpdesk" maken meer slachtoffers in Nederland. Bovendien weten ze daarbij ook flink meer geld buit te maken. Het aantal meldingen, de hoeveelheid slachtoffers én de geleden verliezen groeien flink, blijkt uit nieuwe cijfers van de Fraudehelpdesk.

Vorig jaar al 2 ton
De Fraudehelpdesk is een Nederlandse non-profit die burgers en bedrijven wil behoeden voor oplichtingspraktijken. Het verzamelt hier ook meldingen over, waar nu een zorgwekkende ontwikkeling uit blijkt. Begin maart wist de Fraudehelpdesk al te melden dat zogenaamde Microsoft-bellers vorig jaar minstens 102 Nederlanders te grazen hebben genomen. Mensen worden gebeld met een overtuigend verhaal dat hun computer geïnfecteerd is met malware, waarna de oplichters uiteindelijk de controle over de pc proberen te krijgen en internetbankieren willen kapen.
In totaal zijn er vorig jaar 1403 meldingen gedaan, waarvan dus 102 mensen daadwerkelijk geld zijn kwijtgeraakt aan de oplichters. De totale schade door onder meer frauduleuze overboekingen bedroeg bijna 204.000 euro. Uitschieter was één slachtoffer die maar liefst 47.000 euro afhandig is gemaakt. De trend zit in de lift, blijkt uit de nieuwste cijfers over 2017 die de Fraudehelpdesk nu heeft verstrekt.

Flink meer schade
De fraudeurs blijken in de eerste paar maanden van dit jaar al succesvoller dan ze in diezelfde periode vorig jaar waren. Voor de periode van januari tot half mei ligt het aantal meldingen al op 685 stuks, het aantal slachtoffers op 60 en de schade op 181.958 euro. Ter vergelijking: in januari tot half mei 2016 waren er 747 meldingen, 45 slachtoffers en 52.127 euro aan schade.
Opvallender nog is dat de eerste vierenhalve maand van 2017 qua schade al het jaartotaal van 2016 nadert. De teller staat op net niet de helft voor het aantal meldingen, op bijna tweederde voor het aantal slachtoffers, en op bijna negentiende van de buit. De Fraudehelpdesk spreekt van een "significant hoger schadebedrag" en noemt als mogelijke oorzaak dat de oplichters zelf geld wegsluizen, maar mogelijk ook ransomware op de gekaapte pc van hun slachtoffers zetten.

Link met WannaCry
Deze nieuwe activiteit van 'de Microsoft-helpdesk' is niet de recente uitbraak van ransomwareworm WannaCry. Toch valt er een link te leggen met die beruchte malware. National Technology Officer Hans Bos van Microsoft Nederland verwacht namelijk een nieuwe golf van telefoontjes. Juist de wereldwijde aandacht die WannaCry heeft getrokken, ook in algemene media, versterkt de geloofwaardigheid van de alarmerende 'Microsoft-telefoontjes'. "Er komt waarschijnlijk een piek aan", voorspelt Bos.
De telefonische oplichters, die na het ompraten van slachtoffers dan via internet hun slag slaan, maken misbruik van 'de goede trouw' van mensen. Het gaat om mensen die zich zorgen maken over computersecurity, wat op zich een terechte zorg is, aldus Bos. Hij benadrukt dat dit soort telefoontjes volledig nep zijn: "Microsoft neemt sowieso nooit spontaan, ongevraagd contact met je op."

Hang op, klik weg, doe aangifte
De echte Microsoft-helpdesk zou dit pas doen nadat een gebruiker eerst zelf heeft gebeld of gemaild. Het officiële advies vanuit Microsoft is dan ook: "Hang op, klik weg, en doe aangifte." Bos benadrukt die laatste stap, die uiteindelijk moet helpen om deze fraudevorm breder aan te kunnen pakken. Zonder aangiftes lijkt er immers geen groot probleem te bestaan, terwijl de cijfers van de Fraudehelpdesk toch een stijgende lijn aangeven.
Daarnaast kan Microsoft zelf deze fraude pas bestrijden als het 'direct benadeelde' is. Aan dat juridische criterium wordt pas voldaan als een frauduleuze helpdesk zich bewijsbaar voordoet als Microsoft, dus bijvoorbeeld een webpagina gebruikt met daarop het logo van Microsoft. "Heel flauw", verzucht Bos over deze juridische realiteit.

Zaak bouwen
"Daarom is het juist zo belangrijk dat slachtoffers aangifte doen", herhaalt hij. "Daarin kan namelijk worden aangegeven of de fraudeur zich letterlijk en direct als Microsoft-medewerker heeft voorgedaan. Dit soort punten maken de juridische feiten." Bos legt uit dat Microsoft soms wel actie kan ondernemen, zoals laatst in de Verenigde Staten is gedaan samen met de overheid. Verder doet het softwarebedrijf aan informeren, assisteren en waarschuwen. Hiervoor heeft het een internationale actie lopen met onder meer een meldingssite en uitleggende blogposts.

INDEX

Politie doet weinig met aangifte online-oplichting

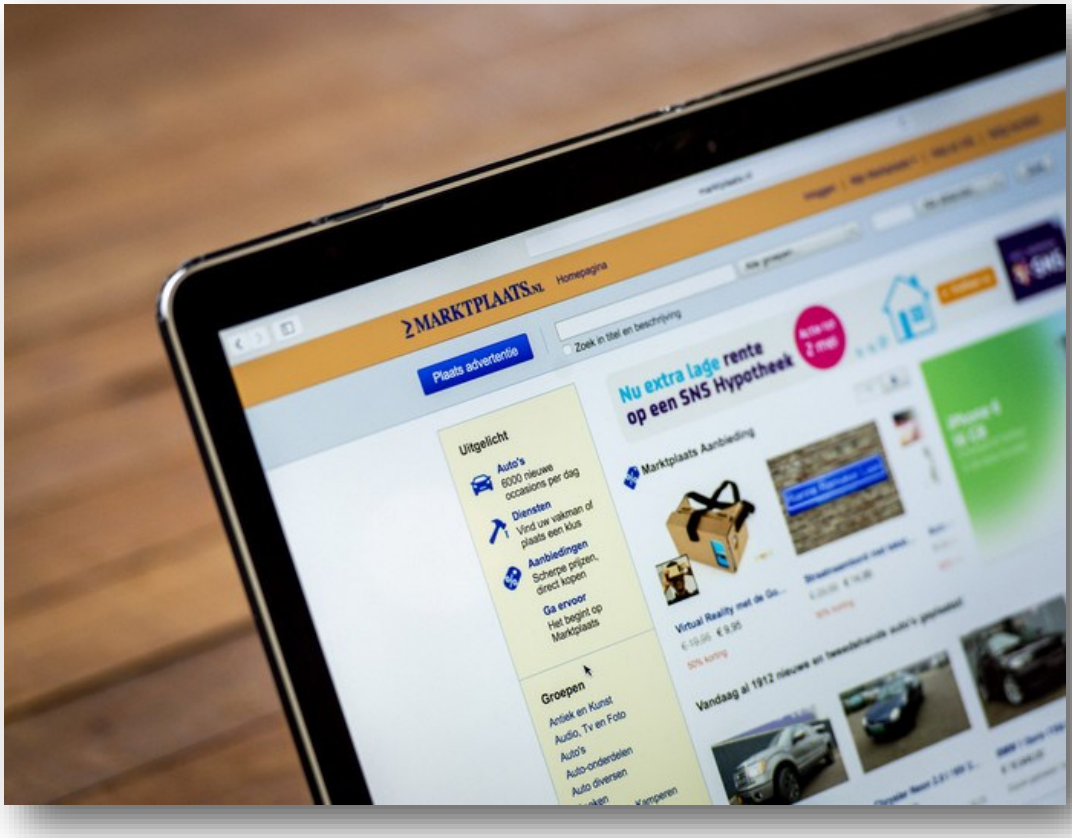
Mensen die via internet een product hebben gekocht maar dat niet hebben ontvangen, krijgen bijna nooit hun geld terug.

Volgens het Centraal Bureau voor de Statistiek werden er in 2016 ongeveer een half miljoen mensen het slachtoffer van koopfraude. De meeste fraude vond plaats in de categorieën 'tickets en kaartjes', '(spel) computers en software' en 'kleding en accessoires'. In ongeveer de helft van de gevallen ging het om een bedrag van meer dan 100 euro en werd de aankoop via Marktplaats gedaan.

Van de mensen die tevergeefs moesten wachten op een besteld product, zegt ruim 9 op de 10 hun geld definitief kwijt te zijn. De gedupeerden zijn vooral ontevreden over de afhandeling van hun aangifte door de politie. Veel deelnemers aan het publieksonderzoek doen wel aangifte, maar dit levert bijna nooit iets op.

Onvoldoende capaciteit
Een groot deel van de gedupeerden kreeg te horen dat er meerdere aangiftes nodig zijn of dat het bedrag te laag was voordat de politie er iets mee doet. Anderen kregen het bericht dat er geen onderzoek wordt gestart, omdat de aangifte 'niet voldoet aan de voorwaarden' of omdat er 'onvoldoende capaciteit' is.

De politie bevestigt tegen de NOS dat lang niet alle aangiften leiden tot een onderzoek en dat er pas een onderzoekt wordt gestart wanneer er meerdere aangiften tegen een persoon of bedrijf binnenkomen. Vorig jaar leidde 1 op de 5 aangiften tot een strafrechtelijk onderzoek. Er werden 346 onderzoeken gestart, 500 verdachten geïdentificeerd en 1700 bankrekeningen geblokkeerd.



INDEX

Tips om je wifi te beveiligen

Standaardfout
Elke router komt standaard met inloggegevens; als ze al beschikken over een wachtwoord. Het beste dat je kan doen, is ze meteen aanpassen. De generische inloggegevens zijn vrij verkrijgbaar op het internet, waardoor je ze evengoed achterwege kan laten. Fabrikanten gebruiken ze alleen zodat je ze meteen zou aanpassen de eerste keer dat je inlogt op een router. Heb je een slecht geheugen, dan kan het geen kwaad ze te noteren op een briefje dat je onder de router legt; als een inbreker het daar vindt, heb je grotere zorgen dan een lek wifinetwerk.

Netwerknaam
De Service Set Identifier (SSID) is de naam die uitgezonden wordt vanaf je router om zichzelf bekend te maken. Op die manier weten mensen welk netwerk van hen is en kunnen ze makkelijk inloggen. Het is belangrijk dat je die naam meteen personaliseert, samen met je inloggegevens. Fabrikanten gebruiken namelijk vaak hun merknaam en het typenummer van de router als SSID. Voor ongewenste bezoekers is het dan een koud kunstje om snel op te zoeken wat de standaardinloggegevens zijn voor jouw model.

Gebruik encryptie
Met encryptie bedoelen we het wachtwoord waarmee je een toestel verbinding kan laten maken met een router. Dat is dus nog iets anders dan de inloggegevens die je eerder al wijzigde. Bij voorkeur gebruik je WPA2; een standaard die aanwezig is op elke moderne router van de afgelopen tien jaar. Is dat niet het geval, dan kan je WPA gebruiken, al is die encryptie veel makkelijker te breken. Gebruik een wachtwoord dat niet te makkelijk is, zoals een nonsensicale wachtwoordzin: die kan je onthouden en kan niemand anders ooit raden.

Vermijd gastnetwerken
Gastnetwerken zijn handige hulpmiddeltjes om vrienden en kennissen snel op je wifinetwerk te krijgen, zonder dat ze veel schade kunnen aanrichten of kunnen binnenkijken in de rest van je netwerk. Helaas maken ze het ook voor buitenstaanders erg makkelijk om binnen te geraken. Het is daarom een veel beter idee om je bezoekers te vertrouwen met het wachtwoord, het voor hen in te toetsen, of het nadien gewoon te veranderen.

Updaten
Zoals je smartphone of tablet steeds beter gaat werken wanneer hij regelmatig updates krijgt, zo zal ook je router beter worden. Fabrikanten sturen regelmatig verbeteringen uit, maar we zijn met zijn allen te lui om die meteen (of ooit) uit te voeren. Nochtans verbeter je niet alleen de werking van je toestel, maar voeg je ook broodnodige beveiligingswerken uit. Geen enkel toestel is perfect, maar het kan dat wel worden als je regelmatig updatet. Voor de echte kenners zijn er overigens software-oplossingen te vinden van derde partijen, al kan niet elke router dat zomaar aan. Google eens naar Tomato, DD -WRT of OpenWrt.

Blokkeer WPS
Wi-Fi Protected Setup (WPS) is een makkelijke manier om je toestellen snel te verbinden met je netwerk. Zelfs wanneer je een wachtwoord hebt ingesteld, kan je door deze knop in te drukken meteen verbinding maken. Leuk en handig, maar mogelijk ook gevaarlijk. Iedereen met toegang tot je router kan de beveiliging zo in een handomdraai kraken, en dat wil je liever niet. Tenzij je je router in een kluis hebt staan – wat niet aan te raden is voor een goede verbinding – schakel je WPS best uit.

Minder energie
Overal in huis een sterk signaal ontvangen, is de droom van iedereen. Als je router zich op een appartement bevindt, ergens in een hoekje, betekent dat echter dat je buren eveneens je perfecte wifisignaal kunnen ontvangen. Het is dan geen slecht idee om je signaal wat zwakker te maken. Het klinkt onlogisch, maar zolang je overal nog verbinding kan maken, heb je al genoeg. In de instellingen van je router kan je het energieniveau laten zakken naar pakweg 75 procent. Je zal nog steeds een snelle verbinding krijgen, maar je buren zullen er niet van kunnen profiteren.

VPN
Een Virtual Private Network (VPN) graaft een tunnel van je toestel naar het internet via de server van een externe partij. Op die manier kan je je identiteit verbergen of jezelf voordoen alsof je in een ander land bent. Dat is handig voor Netflix, maar het is ook veilig. Als je verkeer onderschept wordt, is het bijna onmogelijk om de encryptie van je verbinding te ontcijferen en je data uit te lezen.

INDEX

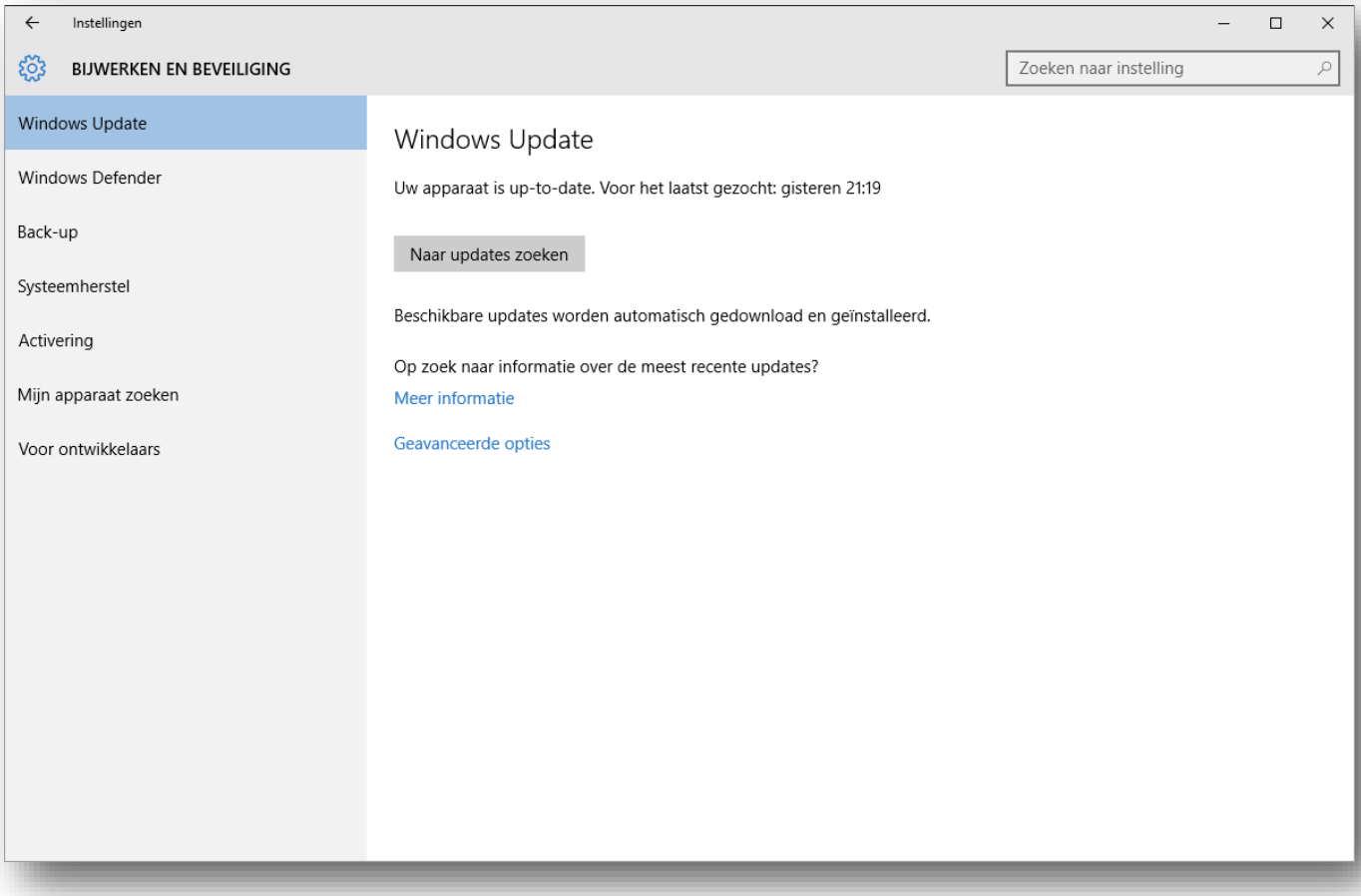
Windows handmatig updaten

Om te zorgen dat je computer goed beveiligd blijft, is het belangrijk om je programma's en besturingssysteem regelmatig te updaten. Windows 10 kan automatisch updates installleren. Maar soms is het beter om dit tussendoor ook even zelf handmatig te doen. Windows handmatig updaten doe je zo.

Automatische updates van Windows zijn handig omdat je op die manier nooit per ongeluk vergeet om je systeem up-to-date te houden. Dagelijks wordt er op de achtergrond gecheckt of er nieuwe updates beschikbaar zijn voor Windows en andere Microsoft producten die op je computer staan. Deze updates worden wanneer dit kan meteen geïnstalleerd. Voor sommige updates moet je je pc opnieuw opstarten. Wanneer er bijvoorbeeld een beveiligingslek ontdekt is of wanneer er zoals vorige week een grootschalige cyberattack wordt uitgevoerd, kun je Windows beter meteen handmatig updaten in plaats van te wachten tot de volgende automatische update.

Windows handmatig updaten
Om zelf naar de Windows Update tool te navigeren, moet je Instellingen > Windows Update gaan en op Naar updates zoeken klikken. Vervolgens wordt er meteen naar nieuwe updates voor je systeem gezocht die nog niet geïnstalleerd zijn.

Om veiligheidsredenen is het in Windows 10 Home niet mogelijk om updates te verbergen, zodat je niet per ongeluk een belangrijke update overslaat. In Windows 10 Pro kan dit wel, dus let goed op dat je geen belangrijke updates verborgen hebt.
Installeer alle gevonden updates en start vervolgens je pc opnieuw op. Het is een goed idee om daarna opnieuw naar Instellingen > Windows Update te gaan en nogmaals naar updates te zoeken. Sommige updates kunnen namelijk betrekking hebben op een update die je zojuist geïnstalleerd hebt en daarom nog niet zichtbaar waren toen je die update nog niet had.



INDEX

Binnenkort geen laptop meer in het vliegtuig naar de VS?

Voortaan mag je mogelijk geen laptops en tablets meer meenemen als handbagage op vluchten naar de Verenigde Staten. Dat leerde The Daily Beast van bronnen bij de Europese veiligheidsdiensten. De Verenigde Staten zouden immers van plan zijn om het elektronicaverbod op vliegtuigen uit te breiden naar Europa. Daardoor zou alle elektronica die groter is dan een smartphone vervoerd moeten worden in het laadruim.

Er is nog geen officiële aankondiging, maar naar verluidt zou die later op de dag volgen. Volgens bronnen van The Daily Beast zou het verbod mogelijk al volgende donderdag ingaan. Ook de Europese Luchthavenorganisatie ACI Europe stuurde al een mail naar luchthavens dat het verbod binnen enkele dagen zal worden aangekondigd, aldus VTM Nieuws. Het verbod zou dan 72 uur na de officiële aankondiging van kracht gaan.

Wat zou er concreet veranderen?

Alle elektronische apparaten die groter zijn dan een smartphone zullen niet meer toegelaten worden bij vluchten naar de Verenigde Staten. Bij het inchecken zullen reizigers aangespoord worden om hun elektronica in de koffer te steken. Ook op de website zal je een melding op het scherm te zien krijgen. Daarnaast moet er een laatste controle zijn voor de reizigers aan boord gaan, want er zullen ongetwijfeld passagiers zijn die niet op de hoogte zijn van het laatste nieuws.

Smartphones hebben ook batterijen aan boord, maar toch worden die wel toegelaten. De specifieke regels zijn niet helemaal duidelijk. De toestellen mogen niet te groot zijn, maar de Amerikaanse overheid laat het na om er een specifieke grootte op te plakken. Camera's, tablets, e-readers, draagbare DVD-spelers, spelconsoles, reisprinters en scanners zijn ondertussen wel verboden.

Waarom?

Het Amerikaanse elektronicaverbod maakt deel uit van een reeks aan antiterreurmaatregelen. De maatregel gold al voor vluchten uit enkele landen in Noord-Afrika en het Midden-Oosten, namelijk Egypte, Jordanië, Koeweit, Marokko, Qatar, Turkije, de Verenigde Arabische Emiraten en Saoedi-Arabië. Niet toevallig gaat het om landen met een grote moslimbevolking, want de Amerikaanse president Donald Trump is ervan overtuigd dat uit deze landen veel terroristen Amerika willen binnendringen. De regels gelden ondertussen ook al voor het Verenigd Koninkrijk.

Dat Europa aan dat lijstje wordt toegevoegd is niet verwonderlijk, want Europa kent een grote toestroom aan vluchtelingen uit onder meer het Syrische oorlogsgebied. In Amerika wordt Europa daarom aanzien als een broeikast voor mogelijk gevaar. Men vreest namelijk voor explosies op vluchten door batterijen in laptops of tablets. Terroristen zouden explosieven in hun laptop kunnen verbergen.

Geen veiligheidsmaatregel, maar afschrikking

De Amerikaanse burgerrechtenbeweging EFF noemde deze maatregel een stukje theater, want ze doet niets echt om de veiligheid te verbeteren. Integendeel, door de laptop als ruimbagage in te checken kunnen overheidsfunctionarissen ongevraagd toegang tot je toestel krijgen.

INDEX

Wat mag Facebook doen met jouw foto's?

Regelmatig zie je vreemde beweringen opduiken over wat Facebook met jouw informatie en foto's van plan is. Moeten we schrik krijgen of niet?
"Een kennis van mij is advocaat en heeft de waarachtigheid hiervan bevestigd. Post de volgende status op jouw muur, of Facebook mag voortaan jouw foto's verkopen." De volgende zin begint dan doorgaans met "ik verklaar bij deze dat…". Het zijn posts die we regelmatig zien terugkeren op Facebook. Ze verspreiden zich snel en krijgen vaak giftige reacties mee die stellen hoe crimineel het sociale medium wel niet is.
Het is niet helemaal onwaar: veel van wat we uploaden naar Facebook wordt gebruikt op een of andere manier. Wie
de gebruiksovereenkomst uitpluist, krijgt bovendien geen eenduidig antwoord op zijn vragen. Welke rechten heeft Facebook nu echt, en welke rechten heb jij?
Eigendomsrecht
Om te beginnen, een uittreksel uit de gebruiksovereenkomst:
Inhoud en informatie delen
Jij bent eigenaar van alle inhoud en informatie die je op Facebook plaatst en je kunt de privacy - en toepassingsinstellingen gebruiken om te bepalen hoe de inhoud en informatie wordt gedeeld. Verder gelden de volgende bepalingen:
Voor inhoud waarvoor intellectuele-eigendomsrechten gelden, zoals foto's en video's (IE-inhoud), geef je ons specifiek de volgende toestemming met inachtneming van je privacy- en toepassingsinstellingen: je verleent ons een niet-exclusieve, overdraagbare, sublicentieerbare, royaltyvrije en wereldwijde licentie voor het gebruik van IE-inhoud die je op of in verband met Facebook plaatst (IE-licentie). Deze IE-licentie eindigt wanneer je jouw IE-inhoud of je account verwijdert, tenzij je jouw inhoud hebt gedeeld met anderen en zij de inhoud niet hebben verwijderd.
Wanneer je IE-inhoud verwijdert, wordt deze verwijderd op een manier die vergelijkbaar is met het legen van de prullenbak op een computer. Je begrijpt dat verwijderde inhoud echter gedurende een redelijke tijd mogelijk aanwezig blijft in back-ups (maar niet beschikbaar is voor anderen).
Wanneer je een toepassing gebruikt, vraagt de toepassing mogelijk toestemming voor het openen van je inhoud en informatie en de inhoud en informatie die anderen met je hebben gedeeld. We vereisen dat toepassingen je privacy respecteren en je toestemming voor de betreffende toepassing bepaalt de wijze waarop de toepassing deze inhoud en informatie kan gebruiken, opslaan en overdragen. (Lees ons gegevensbeleid en de platformpagina voor meer informatie over het platform, waaronder de wijze waarop je kunt bepalen welke informatie andere personen kunnen delen met toepassingen.)
Wanneer je inhoud of informatie publiceert met de instelling Openbaar, betekent dit dat je iedereen, inclusief mensen buiten Facebook, toestemming geeft om die informatie te bekijken en te gebruiken en deze aan jou te koppelen (d.w.z. je naam en profielfoto).

De inleiding stelt al meteen duidelijk dat jij de eigenaar bent en blijft van alles dat je online zet. Het tweede deel van de zin is eveneens belangrijk: hoe jouw data wordt gebruikt, wat de volgende puntjes ook zeggen, hangt grotendeels af van hoe jij jouw privacy- en toepassingsinstellingen hebt ingesteld. Er hangt dus veel af van je eigen grondigheid op vlak van privacy.
Het eerste puntje stelt vervolgens dat, terwijl jij de eigenaar bent, je Facebook stilzwijgend toestemming geeft om jouw afbeeldingen te gebruiken in een erg ruime licentievorm. Laat ons dat puntje even onderverdelen. De licentie is niet-exclusief: dat betekent dat je vrij bent om je eigen foto's verder te verkopen aan bijvoorbeeld stockafbeeldingenwebsites. Je bent vrij om met jouw foto's te doen wat je wilt en Facebook kan je niets verbieden.
Onzichtbaar
De licentie is overdraagbaar en sublicentieerbaar: Facebook kan jouw foto's gebruiken op zijn volledige platform, waaronder bijvoorbeeld ook Instagram. Dat betekent niet noodzakelijk dat Facebook jouw afbeeldingen zal doorverkopen aan adverteerders of stockwebsites – het zou dat strikt genomen wel kunnen, maar het zal dat niet snel doen uit schrik voor een storm aan kwade reacties.
Deze bepaling is eerder bedoeld om het mogelijk te maken dat jouw vrienden je berichten kunnen zien. Facebook post je afbeeldingen namelijk door naar de feed van je vrienden, maar daar hebben ze jouw toestemming voor nodig. Zonder deze bepaling zou je telkens, per persoon, toestemming moeten verlenen aan je vrienden om de afbeelding te zien. Anders zou je onzichtbaar zijn voor hen. Ook voor het doorposten naar Instagram is deze toestemming vereist.
Royaltyvrij en wereldwijd betekent simpelweg dat Facebook je niet zal betalen telkens een van jouw vrienden je foto bekijkt. Daarnaast kan iedereen ter wereld de foto bekijken indien je privacy-instellingen dat toelaten.
Verwijderen
Wanneer je afbeeldingen of andere gegevens verwijdert van Facebook staat dat gelijk aan het intrekken van de licentie. Facebook mag jouw afbeeldingen niet langer verspreiden, maar, zoals gezegd in punt twee, kan het enkele weken duren vooraleer de afbeelding verwijderd is van elke server. Anderen kunnen er evenwel niet meer aan.
Punt drie geeft verduidelijking over apps die je gebruikt. Van zodra je een app bepaalde toestemmingen geeft, bijvoorbeeld toegang tot jouw foto's, geef je hen dezelfde licentie als degene die je aan Facebook gaf. Opnieuw is die voornamelijk bedoeld om je gegevens te kunnen tonen aan contactpersonen. Voor apps als Instagram is het dan ook vrijwel onmogelijk om de app te gebruiken als je die toestemming niet zou geven.
Juiste instellingen
In punt vier zien we meer informatie over de privacy-instellingen. De verklaring maakt duidelijk dat heel veel afhangt van je instellingen. Zet je alles op 'Openbaar', dan betekent dat dat je iedereen de toestemming geeft om je afbeelding te bekijken en daarbij jouw profiel eraan te koppelen. Uiteindelijk heeft Facebook dus een grote vrijheid met jouw afbeeldingen, maar jij blijft hoe dan ook in bezit en je behoudt de controle over alles dat je online zet.
'Verklaringen van advocaten' heb je dus helemaal niet nodig en, nee, ze werken ook helemaal niet.

Bron: ZDnet

INDEX

Privacy en Wikipedia: Hoe veilig is de online encyclopedie?

Internetencyclopedie Wikipedia is een van de meest bezochte websites ter wereld. Tijdens Wikipedia Day werd begin dit jaar het zestienjarig bestaan van de site uitgebreid gevierd. Maar kan het privacybeleid van Wikipedia ook worden toegejuicht?

Wikipedia is in de basis heel transparant. Niet alleen de software waar Wikipedia op draait, maar ook de inhoud van de internetencyclopedie is voor iedereen inzichtelijk. Bezoekers zien in één oogopslag wie wat heeft geschreven en kunnen een watchlist instellen zodat ze bericht krijgen wanneer bepaalde pagina's worden gewijzigd. Omdat Wikipedia zich profileert als "the encyclopedia anyone can edit" wil je als bezoeker weten of dit ook voor de privacyvoorwaarden geldt: dat is gelukkig niet het geval.
Wel wordt er sterk rekening gehouden met de mening van websitebezoekers. Nieuw privacybeleid wordt dertig dagen in verschillende talen open gesteld voor eventuele input uit de Wikipediacommunity. Ook kleine wijzigingen in het beleid worden vooraf aangekondigd. Wikipedia biedt dus een goede basis als het om privacy gaat.

Wat opvalt is dat Wikipedia niet draait op basis van advertenties. Er zijn dan ook geen trackers voor reclamedoeleinden, sociale media buttons of cookies van derden actief op de site. Toch word je als bezoeker wel in lichte mate in de gaten gehouden. Volgens het privacybeleid wordt informatie over het apparaat waarmee je de site bezoekt opgevraagd, samen met het type browser en het versienummer daarvan.
Daarnaast worden onder andere je taalinstelling, naam van de provider, de website waar je vandaan kwam, de pagina's die je bezoekt en de datum en tijd van het bezoek opgeslagen.
Wikipedia geeft een helder overzicht van het gegevensbeleid en de bewaartermijnen, maar zou kunnen overwegen bepaalde gegevens zoals e-mailadressen en accountgegevens eerder te verwijderen. Deze worden in de huidige situatie namelijk niet weggehaald na verloop van tijd.

Aan de hand van gegevens zoals de naam van een provider en de onderwerpen waaraan is bijgedragen zou de identiteit van iemand op Wikipedia misschien kunnen worden herleid. Dit lijkt op zich geen probleem bij een kenniswebsite als Wikipedia, maar in sommige landen waar het recht op vrijheid van informatievergaring onder druk staat kan dit heel riskant zijn. In het privacybeleid staat expliciet dat mensen hun echte naam niet hoeven op te geven bij het registeren van een gebruikersnaam. Wel moet het IP-adres worden afstaan.
Volledig anoniem teksten aanleveren is lastig. Zo worden gebruikers van TOR (The Onion Router) geblokkeerd. Wikipedia kiest bij de bescherming van de inhoud voor een privacyvriendelijke optie: door het handhavingsbeleid niet te baseren op persoonsnamen maar op IP-adres worden er zo min mogelijk privacygevoelige gegevens verzameld en kunnen internettrollen worden geweerd.
Het privacybeleid van Wikipedia kun je niet alleen in verschillende talen terugvinden, maar de Wikipedia's van landen zijn ook van elkaar losgekoppeld. Als gevolg hiervan kan bijvoorbeeld de Chinese Wikipedia worden geblokkeerd als de inhoud daarvan in strijd is met het Chinese recht, maar blijft de Engelse versie van Wikipedia gewoon beschikbaar in China.
Zo werd in Rusland een pagina over het maken van hasj ontoegankelijk gemaakt, terwijl deze pagina in Nederland wel beschikbaar bleef. Wikipedia zou dit verschil duidelijker kunnen aangeven op de website. Bezoekers moeten namelijk weten op basis van welk recht de artikelen worden beoordeeld.

Uit de rechtszaak die Wikimedia Foundation tegen de National Security Agency (NSA) heeft aangespannen over onrechtmatige surveillance blijkt wel dat Wikimedia tegen doorgifte van persoonsgegevens op grote schaal is.
Helaas voor Wikimedia was de rechter van oordeel dat de organisatie niet kon bewijzen direct geraakt te zijn door het spioneren van de Amerikaanse overheid. Door rechtszaken aan te spannen, privacyvriendelijk beleid te voeren en persoonsgegevens niet voor de hoogste prijs te verkopen komt Wikimedia Foundation en daarmee Wikipedia op voor de privacyrechten van websitebezoekers.
Er worden dan ook relatief weinig persoonsgegevens uitgewisseld via de site. Wikipedia geeft in het privacybeleid wel aan verplicht te zijn mee te werken met het verstrekken van persoonsgegevens als dat op basis van een rechtelijk bevel of wettelijke plicht moet.

Wikipedia probeert zoveel mogelijk een neutrale encyclopedie te zijn. Dit ondanks bijvoorbeeld pogingen vanuit het Amerikaanse Congres in 2006 om pagina's in verkiezingstijd te herschrijven. Beheerders gebruiken regelmatig de mogelijkheid om IP-adressen te blokkeren. Volgens Wikipedia-criticus Gregory Kohs is de rol van Wikipediabeheerders niet zo neutraal als het lijkt.
Kohs, die werd geblokkeerd omdat hij het verdienmodel van zijn bedrijf op Wikipedia had gebaseerd, stelde dat hij door beheerders in de gaten werd gehouden tot de Thanksgivingmaaltijd bij zijn ouders aan toe. Dit om zijn locatie vast te stellen en daarmee zijn ip-adres te kunnen blokkeren. Kohs is een van de weinigen die kritiek heeft op Wikipedia in de praktijk.
Wat het toekomstige beleid betreft moet Wikipedia erop letten dat technologische vernieuwing een grote impact zal hebben op de privacy. Door opties als voice search open te stellen moet er ook scherp op worden gelet dat het stemgeluid een extra gevoelig persoonsgegeven is dat op tijd moet worden verwijderd.

Conclusie
Wikipedia is een schoolvoorbeeld wat privacy betreft en krijgt een zeer positief eindoordeel . De encyclopedie is zeer transparant over het beleid en er worden relatief weinig bezoekersgegevens verzameld, sommige gegevens kunnen eerder worden verwijderd door Wikipedia.

INDEX

...verder op de website oa .....

CRIMINELEN PROBEERDEN PINAUTOMATEN TE HACKEN

POLITIE DOET ONDERZOEK NAAR DADERS WANNACRY-RANSOMWARE

GOOGLE BLACKLIST SOMMIGE SITES DIE GEBRUIKERS ONVEILIG LATEN INLOGGEN

SLUIT JE PC EENS GOED AF

EXTENSIES INSCHAKELEN IN CHROME'S INCOGNITO-MODUS

CHATPROGRAMMA MET AUTODESTRUCTIE

KEVIN MITNICK GEEFT TIPS OM "ONZICHTBAAR" TE ZIJN OP INTERNET

ZO VIND JE ALLES WAT JE OOIT GEGOOGLED HEBT

.... en meer .....

...verder op de Facebook pagina oa .....

Privacy instellingen; Social media & applicaties

Welke toepassingen gebruiken je webcam?

Bug in bestandssysteem laat Windows eenvoudig crashen

Nog steeds opgelicht via Marktplaats, really?

Waarom moet je hardware veilig verwijderen in Windows?

8 tips om je wifi te beveiligen

BIOS en UEFI: wat je computer doet voor Windows opstart

Van VGA tot USB-C: welke schermaansluiting moet je gebruiken?

.... en meer .....

INDEX

Cops in cyberspace

'Vandaag hebben wij een persoon aangehouden die ons beledigde', schreef de politie Epe op twitter en facebook. De man had op facebook gereageerd op een bericht van de politie https://www.facebook.com/pg/politie.epe/posts/ . Met de tekst 'ACAB' en dat wordt gezien als 'geweld tegen hulpverleners'. Volgens het bericht is er jurisprudentie waaruit blijkt dat lettercombinatie een belediging is. 'Wanneer iemand er voor kiest om deze lettercombinatie op een Facebookpagina van de politie te plaatsen, wordt deze persoon aangehouden'.

———————————————————-

Politie en justitie besteden weliswaar meer aandacht aan het opsporen en vervolgen van internetcriminelen maar eigenlijk nog steeds te weinig. In 2016 behandelde het OM 171 cybercrimezaken, vijftig meer dan in 2015. De afspraak was echter 190 zaken maar dat aantal werd niet gehaald omdat 'politie en OM nog bezig zijn met een noodzakelijke inhaalslag op het vlak van expertise en capaciteit op dit terrein', aldus het OM. Het jaarbericht beschrijft uitgebreid de zaak waarin computerservers in Nederland en Canada werden opgerold, waardoor het dataverkeer van tienduizenden versleutelde Blackberry's zichtbaar werd.

———————————————————

Politieagenten in Vlaardingen hebben gesproken met de 16-jarige jongen en diens vader die 'vreemde privéberichten' stuurde naar de facebookpagina van de politie. De jongen wenste agenten 'ernstige ziektes' toe, aldus een bericht op die facebookpagina. Onderzoek leidde al snel naar de jongen 'We hebben hem duidelijk gemaakt wat de consequenties zijn als we de jongen hadden aangehouden en hij een #strafblad zou hebben gekregen'. De jongen was volgens het bericht zo geschrokken dat hij het nooit meer zal doen. Op verzoek van de agenten bood de jongen excuses aan alle beheerders van de Politie Vlaardingen-pagina aan.

———————————————————-

De politierechter in Leeuwarden heeft 'met de nodige tegenzin' een man (47, uit Hantumhuizen) vrijgesproken van identiteitsfraude. De verdachte had, april 2014, op naam van een ander een account gemaakt bij Kijkshop.nl en daar een tablet besteld. Volgens de officier van justitie was de zaak een schoolvoorbeeld van id-fraude. Maar de wet die dat strafbaar maakt, werd pas mei 2014 ingevoerd. De verdachte pleegde zo een strafbaar feit dat op dat moment nog niet strafbaar was. En dus volgde ontslag van rechtsvervolging.

———————————————————

Geen idee waarom er opeens een file stond. Niemand had gebeld over een ongeluk of zo. Maar op sociale media bleek al snel de reden: er liep een naakte vrouw op de vluchtstrook en foto's daarvan werden snel verspreid. Het incident was voor de politie in San Bernardino County weer eens reden om automobilisten – en andere burgers natuurlijk – te waarschuwen toch vooral eerst 911 te bellen als er iets aan de hand is. Andere korpsen en hulpverleners in de buurt sloten zich bij de actie aan en een heuse campagne was het gevolg: filmen is prima maar eerst de hulpverleners bellen svp. 'In their excitement to document a fire or traffic collision — and be the first to post the photo or video on social media — people are sometimes neglecting to summon help', zei captain Lucas Spelman van de California Fire/Riverside County Fire Department. 'The responsible thing to do is always call the police before you start recording', al was het maar omdat al die sociale media niet 24/7 gemonitord (kunnen) worden.

———————————————————

Nog geen halve dag na de aanslag in Manchester waren de eerste sites online waarop geld werd ingezameld voor nabestaanden en slachtoffers. Dat aantal steeg de afgelopen dagen tot meerdere honderden. Alleen al bij JustGiving zijn er zo'n tweehonderd pagina's, bij vergelijkbare sites eveneens. Het blijkt echter tamelijk lastig om het kaf van het koren te scheiden. JustGiving zegt al het gedoneerde geld 'in quarantaine' te houden tot de inzamelaar gecontroleerd is maar er zijn natuurlijk ook pagina's, vooral op facebook, die overduidelijk van fraudeurs zijn. Action Fraud, zeg maar de Engelse Fraudehelpdesk, geeft daarom tips. 'Spot the signs' is de belangrijkste: let op taalfouten of slecht Engels, op de betrouwbaarheid van de organisatie achter het initiatief.

———————————————————-

Amerikaanse militairen, politieagenten en andere ambtenaren moeten veel voorzichtiger zijn met persoonlijke informatie op internet. Het Office of the Regional Operations and Intelligence Center waarschuwt dat niet alleen cybercriminelen, maar ook extremisten deze informatie kunnen inzetten bij digitale én fysieke aanvallen. Het ROIC noemt vooral datahandelaren een probleem omdat die her en der verzamelde informatie (behalve naw-gegevens ook informatie over koopgedrag en ip-adressen) doorverkopen. Overheidsambtenaren moeten daarom hun 'online voetafdruk' continu monitoren.

———————————————————-

De Belgische Internet Referral Unit is een succes. In het eerste jaar heeft de IRU 174 radicale websites weten te sluiten. In 2016 werden 929 'inbreuken' vastgesteld, waarvan 602 rond terrorisme. Bij de IRU werken nu 21 fulltimers, eind 2017 moeten dat er 33 zijn. Sinds een aantal maanden gaat de dienst ook zelf 'op patrouille' op internet.

———————————————————-

INDEX

Rechtspraak

De rechtbank in Den Haag heeft een man (35, uit Valkenburg, ZH) veroordeeld tot tweeënhalf jaar celstraf (waarvan tien maanden voorwaardelijk) voor het chanteren en afpersen van bezoekers van een datingsite. Verdachte Rutger S. noemde zich online Tina, was zogenaamd op zoek naar mannen. De slachtoffers stuurden naaktfoto's waarmee ze vervolgens werden gechanteerd. De verdachte zou op deze manier maar liefst 54 duizend euro hebben verdiend. Uiteindelijk deden dertig mannen aangifte – terwijl de verdachte in Thailand een luxeleven leidde. Hij werd in 2016 in België opgepakt nadat er een internationaal opsporingsbevel was uitgegeven.

———————————————————-

De rechtbank in Lelystad heeft de man die bekend staat als Hoofdagent Said ter observatie naar het Pieter Baan Centrum gestuurd. 'Said' – echte naam Marciano O. – kreeg in 2016 enige roem op Instagram en facebook met foto's waarin hij in een gestolen politieuniform agenten bedreigde. Hij werd daarvoor veroordeeld; hij kreeg vijf maanden én een klinische behandeling omdat hij ontoerekeningsvatbaar was verklaard. Die behandeling heeft kennelijk weinig effect gehad: de verdachte bedreigde onlangs enkele mensen in Kampen en Ermelo via Whatsapp en Instagram, zou ook wapens inclusief munitie op zak hebben gehad en daarmee iemand hebben bestolen. Zijn rechtszaak stond deze week op de rol maar O. kwam niet opdagen. de zaak is uitgesteld tot juli.

————————————————————

Wel veroordeeld maar geen straf. Een man uit Houthulst, België 'snuisterde' na de scheiding in de e-mails van zijn ex-vrouw. Omdat ze een familieaccount hadden bij hun provider, kon de man na de scheiding haar mail blijven lezen. Dat deed hij vooral toen hij een alimentatieprocedure verloor: in de mails vond hij bewijs dat zijn ex loog over haar inkomsten. De vrouw stapte naar de politie, de man werd gedagvaard voor 'informaticafraude' en het OM eiste een jaar celstraf. De strafrechter vond de man weliswaar schuldig maar legde, onder meer vanwege het blanco strafblad, geen straf op.

In Nederland speelde in 2015 een vergelijkbare zaak: een vrouw die zonder toestemming de mailbox van haar ex-partner doorzocht, mocht die mails wel degelijk gebruiken in haar alimentatie-zaak tegen die ex. Ook al zijn de mails onrechtmatig verkregen en maakte de vrouw inbreuk op de privacy van haar ex, vond de rechtbank dat het maatschappelijk belang van de waarheidsvinding zwaarder woog dan het belang van uitsluiting van onrechtmatig verkregen bewijs.

———————————————————-

Het gerechtshof Leeuwarden heeft in hoger beroep twee mannen veroordeeld tot vijf jaar celstraf plus tbs voor het seksueel misbruiken van een 10-jarig meisje. De verdachten Auke V. en Antonius van 't H. (38 en 63, beiden uit Pingjum) maakten opnames van het misbruik en verspreidden die via internet. Ze werden in 2014 opgepakt nadat de FBI (in 2013) een wereldwijd opererend kinderpornonetwerk blootlegde. In dat netwerk deelden meer dan 45 duizend leden meer dan 360 duizend afbeeldingen. Twee andere Nederlandse verdachten kregen eerder dertig maanden respectievelijk achttien maanden plus tbs.

———————————————————-

In Cardiff, Wales is een man die IS-strijders hielp hun onlinesporen weg te poetsen, tot acht jaar celstraf veroordeeld. Samata Ullah (34) beheerde onder meer een website met instructievideo's over digitaal bewijs. De aanklagers noemden hem een cyberterrorist: vanuit zijn slaapkamer onderhield hij een 'one stop shop' voor terroristen, met vooral tips en trucs om uit handen van de opsporingsdiensten te blijven. Zonder al te veel succes overigens: het meest bekeken filmpje op zijn site scoorde nauwelijks duizend views. Bewijs tegen Ullah werd niet op de site gevonden, dat had hij allemaal goed beveiligd. Ook niet op zijn computer of smartphone. Maar wel op zijn **'usb-manchetknopen'** – die bevatten alle documenten, foto's en filmpjes op basis waarvan hij nu veroordeeld is .

————————————————————

De rechtbank Oost-Brabant heeft een man (52, uit Helmond) veroordeeld voor eigenrichting. 'Wraakvader' Mario Haazen is volgens de rechtbank schuldig aan zware mishandeling met voorbedachten rade en moet daarvoor tien maanden de cel in. De verdachte werd vrijgesproken van poging tot moord of doodslag. Januari jl nam hij wraak op de vermeend online belager van zijn minderjarige dochter. Deze Jack S. (46) deed zich online voor als Jessie en had via Instagram contact gelegd met Mario's dochter. Het meisje kreeg onder meer bloemen thuisbezorgd. Vader Mario vertrouwde het niet en belde de politie. Toen die volgens hem te weinig deed, startte Mario zelf een speurtocht, vooral op facebook, naar de vermeende stalker. De politie adviseerde nog dat vooral niet te doen – er liep al een onderzoek tegen S. – maar de verdachte zette zijn zoektocht toch door. Als de eigenaar van een Hema-filiaal in Asten hem een dag later een usb-stick met camerabeelden geeft waarop te zien is hoe S. chocola koopt, wordt deze snel herkent. Nog meer tips leiden Haazen naar de verblijfplaats van Jack. Als hij diens auto ziet staan, appt hij naar de wijkagent dat hij de auto gevonden heeft. Haazen wacht net zo lang totdat Jack naar buiten komt, rijdt hem achterna en mept hem enkele keren met een sneeuwschep. Hij meldt zich vervolgens op het politiebureau waar hij wordt aangehouden en vastgezet. Tegen de verdachte, die op tv spijt betoonde had het OM zes jaar celstraf geëist. De rechtbank noemt zijn gedrag 'volstrekt onacceptabel' maar vond poging tot moord niet bewezen. De verdachte moet het slachtoffer wel 1925 euro schadevergoeding betalen.

INDEX

Verschijningsvorm cybercrime	138ab *lid 1*	138ab *lid 2*	138ab *lid 3*	138b	139c *lid 1*	139d	139e	161 *sexies*	161 *septies*	350a *lid 1*	350a *lid 2*	350a *lid 3*	350b *lid1*	350b *lid2*
• Malware														
Malware maken en/of verspreiden	X					X		X	X	X	X	X	X	X
Malware (Trojaanse paarden) gebruiken	X	X			X			X	X	X	X	X	X	
• Computerinbraak														
Computerinbraak (hacking)	X		X								X			
Computerinbraak vervolg-handelingen		X	X		X	X	X	X	X	X	X	X		
Portscan						X								
Spoofing/cache poisoning	X	X		X	X	X	X	X		X	X			
Sniffing					X	X	X			X				
Draadloze netwerken hacken/ misbruiken	X	X	X	X	X		X	X		X	X			
Password guessing	X			X		X								
• Website aanvallen														
Veroorzaken open relay									X				X	
Wederrechtelijk open relay gebruiken	X							X		X				
Defacing/vernielen website	X							X	X	X			X	
Defacing/doorleiden internet-verkeer	X							X	X	X				
Cross-site scripting	X	X			X	X	X	X		X			X	
SQL-injecties	X	X						X		X				
• Botnets														
Botnet bouwen en beheren	X	X	X		X					X		X		
• Denial of Service														
DDoS-aanval				X				X		X			X	
• Social Engineering														
Phishing		X			X		X							
Vishing/Smishing		X			X									
• E-mail gerelateerd														
Wederrechtelijk open mail relay gebruiken	X							X	X	X				
Spamming (met DoS tot gevolg)				X				X	X				X	

INDEX

Wetsartikel

Art. 138ab, lid 1 Sr Hacken: opzettelijk en wederrechtelijk binnendringen van een geautomatiseerd werk

Art. 138ab, lid 2 Sr Hacken: overnemen, aftappen of opnemen van gegevens uit een geautomatiseerd werk na binnendringen daarvan

Art. 138ab, lid 3 Sr Hacken door tussenkomst van een openbaar telecommunicatienetwerk

Art. 138b Sr Het belemmeren van toegang tot of gebruik van een geautomatiseerd werk

Art. 139c Sr Het aftappen of opnemen van gegevens (afluisteren)

Art. 139d, lid 1 Sr Plaatsen van opname-, aftap- of afluisterapparatuur; voorbereidingshandelingen

Art. 139d, lid 2 Sr Het ter beschikking stellen of voorhanden hebben van technische hulpmiddelen of toegangscodes bedoeld om het binnendringen van een geautomatiseerd werk, belemmeren van toegang of aftappen te plegen

Art. 139d, lid 3 Sr Zoals in art. 139d, lid 2 Sr, maar met oogmerk gericht op art. 138ab, lid 2 en 3 Sr

Art. 139e Sr Het bezit en verspreiden van gegevens of een voorwerp waarop gegevens staan die door wederrechtelijk aftappen of opnemen zijn verkregen

Art. 161sexies Sr Opzettelijk vernielen etc. van een geautomatiseerd werk of werk voor telecommunicatie; voorbereidingshandelingen

Art. 161septies Sr Vernieling etc. van een geautomatiseerd werk of werk voor telecommunicatie door schuld

Art. 231b Sr Identiteitsfraude

Art. 232 Sr Opzettelijk valselijk opmaken, vervalsen, gebruiken, etc. van betaalpas, waardekaart e.d.

Art. 240b Sr Kinderpornografie

Art. 248e Sr Grooming

Art. 273, lid 2 Sr Bekendmaking bedrijfsgeheimen; heling computergegevens ondernemingen

Art. 273d Sr Schending telecommunicatiegeheim

Art. 317, lid 2 Sr Afpersing door de bedreiging dat gegevens opgeslagen door een geautomatiseerd werk onbruikbaar, ontoegankelijk of gewist worden

Art. 326c Sr Het misbruiken van een publieke telecommunicatiedienst met het oogmerk daarvoor niet volledig te betalen

Art. 350a, lid 1 Sr Opzettelijke vernieling van gegevens die door middel van een geautomatiseerd werk of door telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen

Art. 350a, lid 2 Sr Het feit gepleegd in lid 1 met tussenkomst van een openbaar telecommunicatienetwerk

Art. 350a, lid 3 Sr Opzettelijk gegevens ter beschikking stellen of verspreiden die zijn bestemd om schade aan te richten in een geautomatiseerd werk

Art. 350b, lid 1 Sr Vernieling door schuld van gegevens die door middel van een geautomatiseerd werk of door telecommunicatie zijn opgeslagen, worden verwerkt of overgedragen

Art. 350b, lid 2 Sr Door schuld gegevens ter beschikking stellen of verspreiden die zijn bestemd om schade aan te richten in een geautomatiseerd werk

INDEX

Video

Tek Tok Late Night:

1. Privacy
2. Internetvrijheid
3. Digitale veiligheid
4. High Tech Crime
5. Data in onderwijs
6. Cybersurveillance
7. Techtrends in onderwijs
8. Veilig internetten
9. MKB cyber secure
10. Cyberellende bij Tek Tok
11. Standaarden en keurmerken
12. Operation Hijg Tech Crime
13. Kraak van de Maand

You Tube:

Doe jij het veilig online
Malware
WiFi ontvangst verbeteren
Internetfraude via de telefoon
Documentaire: Veiligheid en privacy
Herken een nep-hotspot
Gebruik wachtzinnen
Drive-by-downloads voorkomen
Hoe herken je een phishing mail
Beveiligd internetbankieren
Privacy—ik heb toch niets te verbergen
Webinar Computercriminaliteit
Mousejack
Gegijzeld door Ransomware. Wat nu?
Telefonische phishing

Help wanted:

Grooming
Sexting
Webcammisbruik
Bedreigd/gechanteerd
Kinderporno
Nepprofiel

INDEX

Handig

Phishing- / valse e-mails melden:

ABN AMRO Bank: valse-email@nl.abnamro.com

ING Bank: valse-email@ing.nl

Rabobank: valse-email@rabobank.nl

SNS Bank: valse-email@sns.nl

ICS- / ABN AMRO creditcards: valse-email@icscards.nl

Tips voor veilig handelen op Marktplaats

Internetoplichting: controleer vooraf de (bank)gegevens van de verkoper via

www.mijnpolitie.nl/miocheck

Komt de verkoper voor op de website Opgelet op internet ?

Malware ID website met info omtrent verwijderen van infecties

PCrisk verwijderingsrichtlijnen voor spyware en virussen

Cookie Verwijderen kennisdatabase voor het verwijderen van adware, hijackers, ransomware, toolbars en pop-ups

Computer woordenboek

Secure Computing Naslag

Veel meer handige tips vindt u op de Secure Computing website.